This Factsheet has been produced to discuss the topic of *File Permissions*, specifically in Microsoft peer-to-peer and Server oriented systems.

The problem with Microsoft's File Permissions strategy

Over the years, Microsoft has done nothing to improve it's flawed, *User-based security* model, and it inevitably causes problems for Network Users who use multiple-file Applications (such as **SmoothPay**) on their operating systems.

The problems basically stem from the fact that Microsoft's <u>default security model</u> applies ownership permissions to the <u>User</u> that creates any File in the system, regardless of access permissions that may have been applied to the Folders in the system.

What this means is, that despite carefully setting up a Shared Folder for access by Users, granting all Users full access to all the Folders and Files, any time a User Deletes and recreates a File in that shared folder structure, THEY TAKE FULL OWNERSHIP AND RIGHTS TO THAT FILE.

If that User happens to be an Administrator, then absolutely nobody with less that Administrative privileges on that machine (or domain if using a Domain Server) can then Delete and Replace that File.

A solution would be to apply *Application-based security* (just like Linux does via Samba shares on a Server - the Files may be explicitly owned by the same User and Group regardless of who actually created the File - no wonder Linux File Servers are becoming ever more prevalent).

There is possibly a means to provide such a facility automatically to Microsoft systems, but as yet this 35 year veteran of computing has yet to see it. Obviously, any simple solution would be invaluable, but not at the effort and probable expense of setting up scheduled jobs and scripts, changing policies etc - all very mucky stuff for experts, let alone people who just want to use their system.

How does this affect SmoothPay?

SmoothPay uses Microsoft's Visual Foxpro 9 development platform, and by default all data is stored in DBF tables - lots of DBF tables!

Each of these tables is represented by one, two or even three Files containing different parts of the data (data, index and memo contents).

SmoothPay is also busily creating General Ledger Import Files, Direct Credit Files, IRD Schedules (up to 5 different files), PDF, XLS, DOC etc Export Files, Emails and more.

Also, when an update is installed, say by an Administrator, then any new Files (including new reports, new data tables etc) sometimes end up owned by the Administrator instead of the Users who require access to the new Files.

Obviously, a problem occurs when a User tries to generate a direct credit or ledger File that was previously created by a higher-privileged User - causing a File permissions error message, or tries to update the structure of a table that they don't have sufficient rights to modify.

So, what do you need to do?

There are a number of different scenarios, all requiring similar actions to resolve this troublesome issue (temporarily):

Peer-to-Peer Networks

A peer-to-peer network is typically used in small offices, where one PC acts as the Server - it collects the emails, has a decent printer attached, and contains the accounting and payroll systems.

These resources (printers and data folders) may be shared across the Network so that other Users have access to them.

If simple File sharing is enabled (the best option), then usually things will go without a hitch, but sometimes it may be necessary to correct File permissions, especially if a User with Administrator privileges typically uses the "Server" and it's Applications, and other Users end up being denied access to Files due to the Administrative User's effective ownership of one or more Files.

Depending on the operating system (this example demonstrates Windows XP - but it's similar for other versions of Windows too), the following action needs to be taken:

- Open *My Computer*
- Navigate to the *Shared Folder*, and Right-click it
- Choose *Sharing and Security...* or *Properties*
- Choose the *Security* tab
- Set *Everyone* (this is a special User name in Windows) to have *Full Control*
- Choose *Advanced*
- Tick the "*Replace permission entries on all child objects...*" (Sub Folders and Files) option and *Apply,* then *OK*
- In some cases you may need to repeat the process using the *Owner* tab, by specifying who should own all the Files in the Shared Folders -
- Bear in mind though that this DOES NOT mean that any new Files will be "owned" by the specified User or Group - new Files will still be owned by the creating User! (*yes, crazy*)
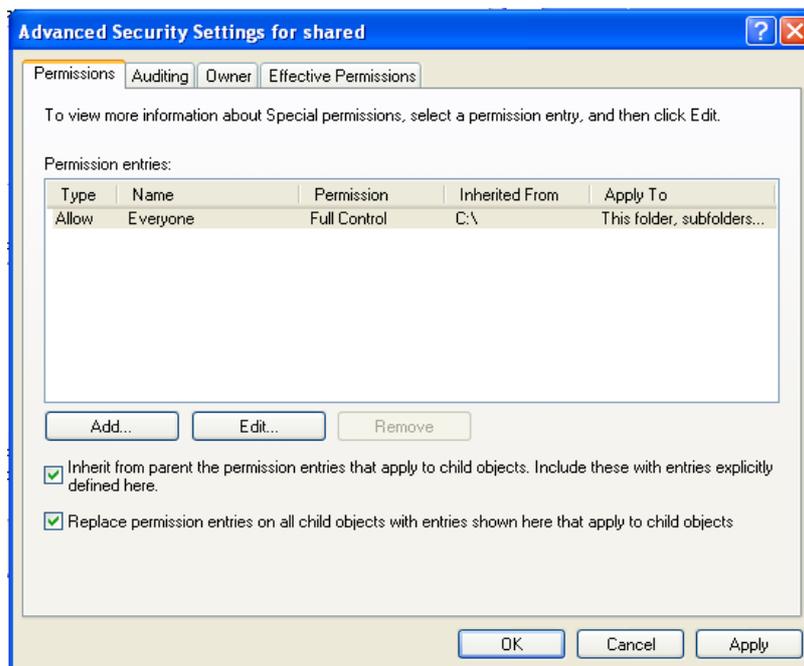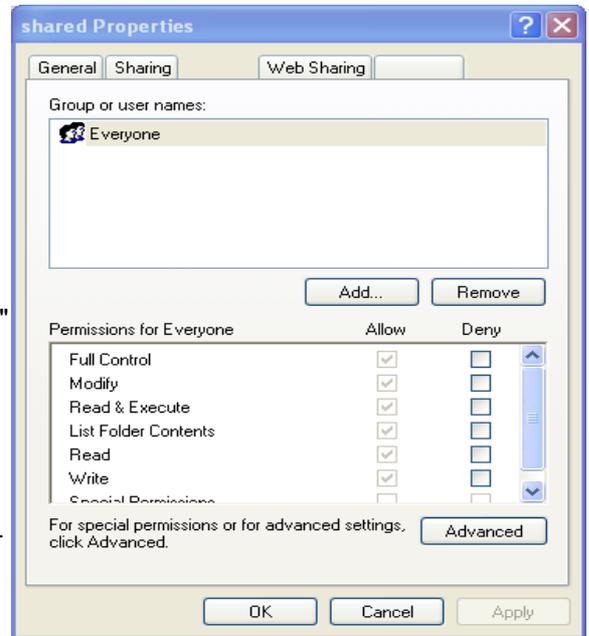
Windows Domain, Server and Normal (Fat) Client

The issues here are exactly the same as those in the peer-to-peer example above, except Domain Users end up owing any new Files created on the Server, unless program installs and updates are performed by a Local Administrator on the Server, in which case the Local Administrator ends up owning any new Files created.

The procedure then, is to reallocate access permissions and probably ownership too so that Users can once again access their Files correctly.

Terminal Services Server and Thin Clients

These system require all installs and updates to be performed using the *Add Remove Programs* utility ON THE SERVER. This is a Microsoft OS requirement, as otherwise any shared libraries (DLLs) and access to File locations will probably not be available to the User.

We've often had discussions with "Experts" who don't really understand the implications of not doing things the Microsoft regulated way, but then they tend to be very small, single-file type Applications where the same issues don't necessarily apply.

Provided the Application has been installed, and updates applied correctly, and that Users have the exact same privilege levels (no Administrators, or otherwise ALL Administrators), then you're unlikely to be affected by permissions issues, though they still may occur too, in which case reallocate access permissions, as in the peer-to-peer example above, so that Users can once again access their Files correctly.

You should not replace ownership unless you are fully aware of the consequences, as such changes undo the security provisions of the *Add Remove Programs* process and the Application may refuse to run.

Citrix Users and Thin Clients

See the example for Terminal Services above.

Citrix Users and PC's Accessing Shares Resources

See the Peer-to-peer example above.

I don't understand anything you just said ...

Networking, just like Payroll, is not for the faint-hearted.

We suggest you use a suitably trained expert to set up and maintain your Network and Installation and updating of your Applications.

Alternatively, install a Linux Server, and don't worry about anything, ever again.

Please call the **HelpDesk** if you require further assistance.

END